

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La preuve et les nouvelles technologies

Mougenot, Dominique

Published in:

La preuve au carrefour de cinq disciplines juridiques

Publication date:

2013

Document Version

le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Mougenot, D 2013, La preuve et les nouvelles technologies. Dans *La preuve au carrefour de cinq disciplines juridiques*. Recyclage en droit, VOL. 2013/3, Anthemis, Limal, p. 161-185.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

La preuve et les nouvelles technologies

Dominique MOUGENOT

Juge au Tribunal de commerce de Mons

Maître de conférences à l'Université de Namur

Maître de conférences invité à l'Université catholique de Louvain

Introduction

Pourquoi parler encore de la preuve et des nouvelles technologies ?

1. La question peut surprendre. Et pourtant, il est révélateur de constater que la quantité de jurisprudence en matière de preuve technologique est inversement proportionnelle à l'importance des écrits qui lui ont été consacrés. La montagne doctrinale et législative a en quelque sorte accouché d'une souris jurisprudentielle. La remarque est particulièrement évidente en ce qui concerne l'acte sous seing privé électronique. Le mécanisme est pratiquement inexistant, tant en pratique que devant les tribunaux. L'acte authentique électronique est sans doute promis à un avenir meilleur, mais peine à décoller. Alors, fallait-il encore parler de l'incidence de la technologie sur les questions de preuve ? En fait, l'examen présente toujours de l'intérêt, pour autant qu'on prenne la peine de voir où se situent les vrais problèmes. De quoi parle-t-on devant les tribunaux ? On constatera dès lors que les difficultés sont tout autant liées à la recevabilité de la preuve qu'à sa valeur probante. Le débat se déplace donc. Si, il y a quelques années, les preuves recueillies de manière illégale et déloyale étaient d'office écartées, il n'en va plus de même aujourd'hui avec le développement de la jurisprudence *Antigone*. La question de la recevabilité devient délicate. Quant à celle de la valeur probante, elle est plus rarement évoquée devant les tribunaux. Heureusement, pourrait-on dire, parce que l'appréciation de la valeur probante de mécanismes technologiquement sophistiqués est délicate pour le juge et passera souvent par des expertises coûteuses.

Section 1

L'acte sous seing privé électronique

§ 1. Généralités

2. Un acte sous seing privé est un écrit établi par des particuliers et signé par eux. Il est donc composé de deux éléments : l'écrit et la signature. La réa-

lisation d'un acte sous seing privé électronique a longtemps été le défi à la fois des commentateurs et du législateur. La difficulté consistait à faire entrer les actes dématérialisés dans les catégories classiques de l'écrit et de la signature, qui avaient été conçues bien avant l'âge de l'informatique. Le problème était plus conceptuel que législatif, puisqu'il n'existait en Belgique aucune définition légale de l'écrit et de la signature.

Pour penser le cadre juridique des technologies nouvelles, deux options étaient possibles. Soit on créait un régime légal de toutes pièces, qui ne s'applique qu'aux mécanismes et documents électroniques et se juxtapose au régime existant, qui continue à s'appliquer aux mécanismes et documents traditionnels, soit on essayait de trouver un régime juridique technologiquement neutre, susceptible de s'adapter aussi bien à l'environnement traditionnel qu'à l'environnement électronique.

Les deux formules ont leurs avantages et leurs inconvénients.

La première a le mérite de tailler une cote parfaitement adaptée à l'électronique. Les spécificités de l'informatique sont prises en compte, ce qui évite les difficultés et hiatus qui peuvent apparaître quand on essaye d'appliquer des règles qui n'ont pas été conçues au départ pour fonctionner dans un environnement électronique. Il s'agit cependant d'une solution lourde, qui oblige le législateur à réécrire un corps complet de dispositions légales. Il appartient alors au praticien de déterminer laquelle des deux législations, traditionnelle ou électronique, doit être appliquée, et des difficultés d'appréciation de leur champ d'application respectif peuvent apparaître. Quoique cette méthode ait de fervents défenseurs¹, elle reste peu utilisée.

La seconde a, au contraire, le mérite de la légèreté : il suffit de retravailler les dispositions incompatibles avec l'électronique pour leur donner une formulation plus neutre sur le plan technologique. La même loi peut alors s'appliquer indifféremment dans les deux environnements. On peut aussi utiliser des « dispositions transversales », qui définissent une règle unique, susceptible de s'appliquer de manière uniforme dans différentes législations. La difficulté de cette méthode réside dans le fait qu'il n'est pas toujours aisé de trouver une formulation des dispositions légales qui épouse aussi bien les caractéristiques de l'environnement traditionnel que celles de l'environnement électronique. La règle nouvelle ne fonctionne pas toujours convenablement, parce qu'elle ne

s'adapte pas complètement aux spécificités de l'informatique et de l'électronique. Ou alors, elle crée un sentiment de frustration, parce qu'elle ne permet pas de tirer profit de toutes les fonctions de l'électronique, qui peuvent être plus nombreuses et plus variées que celles du support papier et de l'environnement traditionnel². Cette méthode est couramment désignée comme celle des « équivalents fonctionnels ». En effet, elle se fonde sur une analyse des fonctions remplies par les concepts ou mécanismes traditionnels (écrit, signature, copie, envoi recommandé...), puis opère une transposition des règles juridiques qui gouvernent ces concepts ou mécanismes à tous les concepts ou mécanismes électroniques qui remplissent les mêmes fonctions. Par exemple, le régime juridique de la signature est transposé à tous les mécanismes électroniques qui remplissent les mêmes fonctions que la signature manuscrite. C'est la méthode la plus utilisée. Elle a servi de modèle à beaucoup de législations ou projets de législation sur l'écrit et la signature électronique, ainsi que sur le commerce électronique, en ce compris en Belgique.

La conception fonctionnelle prévaut actuellement dans notre droit. L'acte sous seing privé électronique a la même force probante qu'un acte sous seing privé traditionnel (article 1322 du Code civil). Il est recevable chaque fois que le Code civil exige une preuve écrite par acte sous seing privé. Dans les domaines où la preuve est libre, toute forme de document électronique, même non signé (e-mail, SMS, tweet...), peut être admise comme preuve. Le juge apprécie librement sa valeur probante.

§ 2. L'écrit électronique

3. L'écrit n'était pas défini en droit, ce qui, en théorie du moins, devait ouvrir largement la porte à l'écrit électronique. Le problème, dans une approche fonctionnelle, était de définir les fonctions de l'écrit. Selon l'exposé des motifs de la loi belge du 20 octobre 2000, relative à la signature électronique, les fonctions de l'écrit sont au nombre de trois³ :

- inaltérabilité : le document ne peut être modifié, volontairement ou involontairement, par les parties ou par des tiers ;

² Ainsi, la signature digitale permet de protéger efficacement le document qu'elle accompagne contre les modifications du texte, ce que la signature manuscrite ne peut faire que dans une mesure assez limitée.

³ *Doc. parl.*, Chambre, 1999-2000, n° 50-38/006, p. 6. Voy. aussi : E. DAVIO, « Preuve et certification sur Internet », *R.D.C.*, 1997, p. 663 ; J. LARRIEU, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ? », *Cah. dr. Inf.*, 1988, H, n° 17 et 18 ; E. MONTERO, « Internet et le droit des obligations conventionnelles », in *Internet sous le regard du droit*, Jeune Barreau de Bruxelles, Bruxelles, Larcier, 1997, pp. 31 et s., n° 15 ; Y. POULLET, « Les transactions commerciales et industrielles par voie électronique. De quelques réflexions autour du droit de la preuve », in *Le droit des affaires en évolution. Le juriste face à l'invasion informatique*, Bruxelles, Bruylant, 1996, p. 54 ; Y. POULLET et M. ANTOINE, « Vers la confiance ou comment assurer le développement du commerce électronique », in *Authenticité et informatique*, Bruxelles, Bruylant-Kluwer, 2000, pp. 345 et s., n° 14.

¹ V. GAUTRAIS, « Les contrats en ligne dans la théorie générale du contrat : le contexte nord-américain », in *Commerce électronique : le temps des certitudes*, Cahiers du CRID, n° 17, Bruxelles, Bruylant, 2000, pp. 91 et s., n° 21 ; J. HUET, « Formalisme et preuve en télématique et informatique », *J.C.P.*, 1990, p. 104, n° 2 ; J. HUET, « Aspects juridiques de l'EDI, Échange de données informatisées », *D.S.*, 1991, pp. 181 et s., spéc. 185 ; J. HUET, « Vers une consécration de la preuve et de la signature électroniques », *D.*, 2000, Chron., pp. 95 et s. ; A. RAYNOUARD, « Adaptation du droit de la preuve aux technologies de l'information et à la signature électronique », *Rép. Defrénois*, 2000, pp. 593 et s., n° 12.

- lisibilité : les informations contenues doivent pouvoir être accessibles à la compréhension humaine grâce à un procédé approprié. Selon les auteurs de l'exposé des motifs, cette lisibilité peut être directe ou médiate (en utilisant le dispositif de lecture adéquat) ;
- stabilité : le contenu de l'écrit doit être fixé définitivement au moment de sa rédaction et doit pouvoir être conservé pour une consultation ultérieure.

L'écrit sur papier remplit naturellement ces différentes fonctions. Il est directement lisible et intelligible (pour autant que le langage utilisé soit compréhensible par le lecteur). Il est stable et se dégrade peu, même si on peut le détruire (encore que le papier thermique du téléfax ne soit pas très résistant à long terme). Le support papier rend, en partie du moins, les modifications de l'original visibles ou décelables.

En revanche, l'application de ces fonctions aux documents sur support électronique (disque dur, disquette, cédérom, DVD...) pose problème. Les informations figurant sur ces supports ne sont lisibles que moyennant utilisation d'un appareil (ordinateur) et d'un logiciel. La durabilité des supports électroniques n'égale pas celle des supports papier et est, en outre, tributaire de l'obsolescence technologique : les logiciels qui permettent de lire un document existant-ils encore dans quelques années ? Ces difficultés ne paraissent toutefois pas constituer un obstacle insurmontable à la reconnaissance de la qualité d'écrit. L'inaltérabilité est beaucoup plus embarrassante. En effet, par nature, un fichier informatique peut être aisément modifié, pratiquement sans laisser de trace : dans un texte, on peut supprimer des mots ou des paragraphes ou les déplacer... Seule une protection spécifique résultant, par exemple, de certains procédés de signature électronique (signature digitale) permet de pallier cet inconvénient.

4. Finalement, une définition de l'écrit est apparue en droit belge en 2003. Le législateur a voulu faciliter les échanges et le commerce électronique en adoptant la loi 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, qui transpose en droit belge la directive du 17 juillet 2000⁴. Cette loi contient une définition de l'écrit électronique. Elle adapte le formalisme contractuel de manière à permettre aux actes électroniques d'y répondre. Le formalisme probatoire est également concerné. La loi du 11 mars 2003 garantit l'équivalence entre l'écrit électronique et l'écrit papier. L'article 16, § 2, de cette loi dispose que l'exigence de l'écrit est satisfaite par « une suite de signes intelligibles et accessibles pour être consultés ultérieure-

ment, quels que soient leur support et leurs modalités de transmission ». On constate que deux des fonctions évoquées ci-dessus, la lisibilité et la durabilité, sont reprises. Plus exactement, il est question d'intelligibilité, ce qui n'exclut pas l'intervention d'un logiciel pour rendre compréhensibles les signes utilisés par la machine. Quant à la durabilité, il est simplement exigé que les signes ne disparaissent pas immédiatement après leur création (à l'extinction de l'appareil, par exemple). En revanche, la condition d'inaltérabilité n'y est pas reprise. Sont donc des écrits : des documents traditionnels sur papier, en ce compris les photocopies et télécopies, mais aussi des documents électroniques (textes créés avec un traitement de texte, courriels, SMS, tweets, textes sur une page web...). Cette disposition vise les hypothèses dans lesquelles l'écrit est requis à titre de condition de forme et concerne notamment le domaine de la preuve (formalisme probatoire). Il y a une telle similitude entre les concepts d'écrits définis dans la loi du 11 mars 2003 et ceux mis en lumière par la doctrine en droit de la preuve que l'on peut raisonnablement admettre que ces notions se superposent⁵. Chaque fois qu'un écrit est requis à titre de formalité, celle-ci peut être considérée comme satisfaite par la production d'un écrit électronique conforme à la définition de la loi.

§ 3. La signature électronique

A. Définition et réglementation

5. Rares sont les sujets qui ont fait couler autant d'encre ! La question de la signature électronique a intrigué les auteurs dès les années 1980. Un des premiers mécanismes à avoir suscité la controverse est l'utilisation simultanée d'un code PIN et d'une carte magnétique. Ces techniques apparaissent actuellement assez sommaires au vu du développement de la technologie.

Le problème est le suivant. Les informaticiens utilisent régulièrement des mécanismes techniques pour authentifier l'origine de documents dématérialisés ou de pages web. Ces mécanismes sont appelés « signature électronique ». Tous ne sont pas reconnus comme des signatures au sens juridique du terme. Pour qu'une signature électronique – au sens technique du terme – constitue également une signature électronique – au sens juridique du terme –, elle doit répondre aux conditions imposées par la loi.

6. La réglementation de la signature électronique en droit belge se retrouve dans deux dispositions ou groupes de dispositions :

⁴ Directive 2000/31/CE du Parlement européen et du Conseil relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, J.O.U.E., n° L178 du 17 juillet 2000.

⁵ D. et R. MOUGENOT, *La preuve*, 4^e éd., Bruxelles, Larcier, 2012, n° 83-2, p. 172 ; P. VAN OMME-SLACHE, « Vers une définition de l'écrit en droit des obligations », in *Liber amicorum Bernard Glansdorff*, Bruxelles, Bruylant, 2008, p. 586.

1. Le Code civil (article 1322) définit la notion de signature électronique en matière de preuve par acte sous seing privé. Cette disposition a été introduite par la loi du 20 octobre 2000, transposant en droit belge la directive sur les signatures électroniques du 13 décembre 1999⁶.
2. La loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification réglemente la signature électronique de manière générale. Son champ d'application est très large, mais inclut aussi le droit de la preuve. Cette loi s'applique à toute utilisation de la signature électronique en droit, en ce compris dans les rapports avec les autorités publiques. Cette loi est également le fruit de la transposition en droit belge de la directive du 13 décembre 1999.
7. L'article 1322 du Code civil se situe dans le chapitre consacré à la preuve et régit les actes sous seing privé. Il précise que la signature peut être constituée par « un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte ». Cet article utilise donc une conception fonctionnelle de la signature. Un ensemble de données électroniques constitue une signature s'il remplit les deux fonctions mentionnées par la loi : 1° permettre l'imputation à une personne déterminée et 2° garantir l'intégrité du contenu. Les travaux préparatoires indiquent que le concept d'imputation à une personne déterminée recouvre en fait à la fois son identification et l'expression de son consentement (« *animus signandi* »)⁷. La loi du 11 mars 2003 sur les services de la société de l'information (article 16) précise que l'exigence d'une signature est satisfaite dès que ces conditions sont remplies. En matière probatoire, le juge peut donc librement apprécier si le mécanisme utilisé par les parties remplit ces deux fonctions. Si la réponse est positive, il est obligé de considérer qu'il a affaire à une signature au sens de l'article 1322 du Code civil.
8. Le législateur s'est avisé de ce que cette disposition, à elle seule, ne transposait pas correctement la directive sur la signature électronique. Le Parlement a donc adopté en outre la loi du 9 juillet 2001, qui met en place un régime général de la signature électronique. Tout d'abord, cette loi donne une définition de la signature électronique, absente dans l'article 1322. Il s'agit d'« une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification » (article 2). La loi établit, en outre, deux principes, repris textuellement de la directive.

⁶ Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire européen pour les signatures électroniques, J.O.U.E., n° L 13, 19 janvier 2000, pp. 12 et s.

⁷ Doc. parl., Chambre, 1999-2000, n° 50-38/006, p. 11.

1. L'article 4, § 5, de cette loi précise qu'« une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif :
 - que la signature se présente sous une forme électronique, ou,
 - qu'elle ne repose pas sur un certificat qualifié ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature ».

Le juge ne peut pas rejeter une signature pour le seul motif qu'elle est électronique ou qu'elle ne répond pas aux conditions de sécurité les plus exigeantes. C'est le principe de « non-répudiation ». Cet article établit donc une règle minimale, mais ne dit toutefois rien des conditions que doit remplir une signature électronique pour être assimilée à une signature manuscrite. C'est le principe suivant qui répond à cette question.

2. L'article 4 de la loi assimile également les formes les plus sécurisées de signature électronique à la signature manuscrite, moyennant le respect de trois conditions : « (1) une signature électronique avancée⁸ (2) réalisée sur la base d'un certificat qualifié et (3) conçue au moyen d'un dispositif sécurisé de création de signature est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale. » La signature qui remplit toutes ces conditions est appelée par la doctrine « signature qualifiée »⁹. En combinant l'article 1322 du Code civil et l'article 4 de la loi du 9 juillet 2001, on arrive à la conclusion qu'une « signature qualifiée » constitue automatiquement une signature valable sur un acte sous seing privé et est présumée remplir les deux fonctions énumérées à l'article 1322.

9. Que retenir de cette réglementation ?

D'une part, le législateur n'a pas voulu limiter le pouvoir d'appréciation du juge en énumérant des mécanismes techniques précis. N'importe quelle technique peut faire l'affaire, pour autant qu'elle réponde aux fonctions mentionnées à l'article 1322 du Code civil.

⁸ La signature électronique avancée, concept repris de la directive, est définie à l'article 2 de la loi comme « une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :

a) être liée uniquement au signataire;

b) permettre l'identification du signataire;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée. »

⁹ Cette appellation est absente dans la loi elle-même.

D'autre part, même s'il n'en fait pas un choix exclusif, le législateur a privilégié un mécanisme particulier, jugé plus performant : la signature digitale. Dans l'état actuel de la technique, c'est le procédé qui répond le mieux aux conditions légales, notamment pour constituer une signature qualifiée. Ce mécanisme se fonde sur la technique de la cryptographie à double clé. L'idée est la suivante. Le message ou une partie de celui-ci est rendu illisible (crypté) en utilisant un code secret propre à l'émetteur (clé). Le destinataire décrypte le message ou la partie cryptée de celui-ci en utilisant un code public, également propre à l'émetteur. Les deux clés (privée et publique) sont mathématiquement liées, de telle sorte que, en décryptant le message avec la clé publique de l'émetteur, le destinataire a la certitude qu'il a été crypté avec la clé privée de l'émetteur. Reste une difficulté : comment être certain, lorsque les partenaires de la communication ne se connaissent pas, que la clé publique est bien celle de l'émetteur ? L'identité du signataire est établie par un certificat, émis par un tiers de confiance (le prestataire de services de certification).

B. Garantie d'authenticité du document électronique

10. Dans l'état actuel de la loi, la signature électronique est le seul procédé explicitement prévu pour garantir l'authenticité d'un acte électronique. L'article 1322 du Code civil prévoit expressément que la garantie de l'authenticité de l'acte sous seing privé électronique est une fonction de la signature électronique, tant en ce qui concerne son origine (« imputé à une personne déterminée ») qu'en ce qui concerne son contenu (« établissant le maintien de l'intégrité de l'acte »).

L'archivage électronique n'est toujours pas réglementé en droit belge et les mécanismes utilisés par l'archiviste n'ont pas de valeur juridique particulière, ni quant à la date des documents conservés ni quant à leur contenu. En pratique, un archiviste qui utiliserait des procédures de conservation jugées fiables pourrait convaincre le juge de l'authenticité des documents qu'il détient, mais le juge conserve une entière liberté d'appréciation à ce sujet.

C. Transmission du document électronique

11. La loi ne réglemente pas, de manière générale, les modes de transmission des actes électroniques. On peut déduire des principes généraux qu'un mode de transmission qui ferait disparaître la signature électronique (suite à l'impression du document sur papier, par exemple) ne permettrait pas de maintenir le statut d'acte sous seing privé d'un acte¹⁰.

La loi du 6 avril 2010 relative aux pratiques du marché et à la protection des consommateurs, dans le cadre de la réglementation des contrats à distance, oblige les entreprises à communiquer certaines informations au consommateur sur un *support durable*. Un tel support doit permettre de stocker les informations adressées au consommateur « d'une manière permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées » (article 2, 25°). Il est admis que ce concept, issu de certaines directives européennes, concerne également des écrits électroniques¹¹. Donc, même si la conclusion de contrats à distance peut se faire autrement que par voie électronique, cette loi impose que, lorsque la communication au consommateur des informations exigées par la loi se fait de manière électronique, elle doit utiliser un tel support durable. Répondent notamment à cette définition : un document enregistré sur un disque dur, une clé USB ou un cédérom ou encore un message électronique adressé au consommateur¹². Ce n'est, en revanche, pas le cas d'une page web publiée sur le site de l'entreprise, qui est trop fugace pour être considérée comme durable¹³.

§ 4. Quels sont les futurs développements de l'acte sous seing privé électronique ?

12. Les développements futurs de la preuve technologique sont encore incertains. Il est évident, avec un recul de plus de dix ans, que la législation sur la signature électronique n'a pas eu le succès escompté. La grande majorité des transactions électroniques est réalisée sans utilisation d'une signature. Dans le commerce électronique, l'utilisation de la signature électronique reste marginale. Le fait de remplir un formulaire avec ses coordonnées, puis de valider la commande, ne peut être assimilé à une signature au sens de l'article 1322 du Code civil : ce mécanisme ne permet pas d'imputer l'opération à une personne déterminée (n'importe qui peut remplir le formulaire). La garantie du contenu de l'acte dépend de la manière dont le site web du prestataire est configuré,

de code-barres, par exemple). La loi du 9 juillet 2001 a été modifiée par la loi du 15 février 2012 pour s'adapter à cette évolution. Le but était de permettre l'émission par les autorités publiques de copies papier de documents signés électroniquement par un fonctionnaire. *Voy. Doc. parl., Chambre, n° 53-1450/001*.

¹⁰ M. DEMOULIN, « La notion de 'support durable' dans les contrats à distance : une contrefaçon de l'écrit ? », *R.E.C.O.*, 4/2000, pp. 361 et s., n° 6 ; E. MONTERO, « La conclusion du contrat à distance », in *Obligations. Commentaire pratique*, Bruxelles, Kluwer, feuillets mobiles, 2007, p. 83 ; D. MOUGENOT, « La preuve - évolution et révolution », in *Le droit des obligations contractuelles et le bicentenaire du Code civil*, Bruges, la Chartre, 2004, pp. 121 et s., n° 65 et s.

¹² *Voy. l'énumération figurant à l'article 1, 17°, de la loi du 27 mars 1995 relative à l'intermédiation en assurances et en réassurances et à la distribution d'assurances, qui utilise le même concept.*

¹³ H. JACQUEMIN, *Le formalisme contractuel - mécanisme de protection de la partie faible*, Bruxelles, Larcier, 2010, n° 279.

¹⁰ Ce dernier point doit toutefois être nuancé, parce que certaines techniques permettent actuellement la vérification de l'authenticité de la signature électronique d'un document même après impression (par un système

ce qui échappe totalement au consommateur. En définitive, c'est le paiement simultané de l'opération qui constitue la meilleure preuve de la volonté du consommateur de passer l'acte. C'est une sorte d'aveu par commencement d'exécution (aveu en action)¹⁴. Ce n'est que dans les rapports entre les banques et leurs clients que des mécanismes de signature sont devenus d'utilisation courante.

La carte d'identité électronique comporte une puce contenant une clé. Assortie d'un certificat, elle permet l'utilisation d'une signature digitale, soit la forme la plus développée de signature, susceptible de bénéficier de la présomption d'assimilation à la signature manuscrite¹⁵. Son introduction a permis d'espérer une généralisation de l'emploi de la signature électronique. Il n'en est rien entre particuliers. L'utilisation de la signature électronique liée à la carte d'identité dans les rapports avec l'administration reste limitée à quelques applications (dépôt en ligne de la déclaration d'impôt, communication de certaines données par les assujettis en matière de sécurité sociale...). Les lois sur la procédure électronique en matière judiciaire (2006), qui auraient fait un usage important de la signature électronique en matière procédurale, ne sont jamais entrées en vigueur¹⁶ par manque d'infrastructure et de développement d'une application permettant le *case management* électronique.

La jurisprudence en cette matière est peu abondante. Les juges sont d'ailleurs mal à l'aise avec les concepts introduits par le législateur en matière de signature électronique¹⁷.

On constate par ailleurs que, alors que le législateur avait privilégié des formes sophistiquées et sécurisées de signature (signature digitale), la pratique voit apparaître des formes assez élémentaires et moins sûres de signature électronique, telles que la signature manuscrite scannée. C'est ce mécanisme qui est utilisé par l'Office des étrangers dans le cadre du contentieux relatif aux refus d'accès au territoire ou d'éloignement des étrangers¹⁸.

Section 2

L'acte notarié électronique

13. Puisque l'acte sous seing privé électronique est un échec, l'acte authentique a-t-il plus de succès ? Il est clair que l'intervention obligatoire d'un officier

public ou ministériel aurait pu provoquer un essor rapide de l'acte électronique, pour autant que les professions concernées fassent le pas de la dématérialisation et dépassent les difficultés propres à l'authenticité de l'acte, et pour autant également que le législateur permette l'utilisation de ce type d'acte. Déjà en France et en Italie, la loi prévoit la possibilité de passer des actes authentiques sous forme électronique¹⁹. De la théorie à la pratique toutefois, le pas est important et les obstacles nombreux.

14. En Belgique, la loi du 11 mars 2003 sur les services de la société de l'information n'a pas apporté d'avancée significative. Elle a créé une ouverture en modifiant l'article 1317 du Code civil, qui dispose désormais que l'acte authentique peut être dressé sur tout support. C'est la porte ouverte à l'acte authentique sur support électronique. Il devrait alors répondre à des conditions fixées par un arrêté royal, qui n'a toutefois pas encore été élaboré à ce jour. Cependant, l'article 3 exclut de son champ d'application les activités de notaire, dans la mesure où elles comportent une participation directe et spécifique à l'exercice de l'autorité publique. En outre, l'article 17 exclut également les contrats qui créent ou transfèrent des droits sur des biens immobiliers, les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique, les contrats de sûretés et garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale, ainsi que les contrats relevant du droit de la famille ou du droit des successions. Tous les actes notariés sont donc exclus du champ d'application de cette loi, soit en raison de la personnalité de leur auteur (intervention d'un notaire en tant qu'officier public) soit en raison de l'objet de ces actes (mutations immobilières, sûretés, libéralités et successions, liquidations de régime matrimonial...). Les assouplissements prévus par cette loi aux problèmes posés par la transposition du formalisme dans un environnement électronique sont dès lors inapplicables en cette matière.

Une loi-programme du 27 décembre 2004²⁰ a permis aux notaires de délivrer des expéditions revêtues d'une signature électronique qualifiée (sur cette notion, voy. ci-dessus n° 8). Cette modification était nécessaire pour permettre d'alimenter les banques de données organisées par les autorités par des documents conformes aux minutes notariales.

¹⁴ D. et R. MOUGENOT, *op. cit.*, n° 286.

¹⁵ O. GOFFARD et E. ROGER-FRANCE, « L'introduction de la carte d'identité électronique en droit belge par la loi du 25 mars 2003 : aspects juridiques », *J.T.*, 2005, pp. 277 et s.

¹⁶ Mis à part quelques dispositions accessoires, entrées en vigueur le 1^{er} janvier 2013.

¹⁷ E. MONTERO, « La signature électronique au banc de la jurisprudence », *D.A.-O.R.*, 2011/98, p. 235.

¹⁸ *Ibid.*, pp. 231 et s.

¹⁹ En France, voy. art. 1317, C. civ., tel que modifié par L. n° 2000-230 du 13 mars 2000, art. 2, (J.O.C.E., 14 mars 2000), et le décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires (J.O.U.E., n° 186, 11 août 2005). En Italie, voy. loi n° 59 du 15 mars 1997, Décrets prés. it., 10 novembre 1997, n° 513, et 8 février 1999.

²⁰ M.B., 31 décembre 2004.

15. Toutefois, le législateur a franchi un pas décisif, en adoptant la loi du 6 mai 2009²¹. Cette loi modifie la loi de ventôse, en spécifiant que les actes notariés peuvent être reçus sous forme dématérialisée. Dans ce cas, l'acte doit être enregistré dans les cinq jours auprès d'une banque des actes notariés (dénommée NABAN), gérée par la Chambre nationale des notaires. Le notaire n'est pas tenu de conserver la minute d'un acte reçu sous forme dématérialisée, après son enregistrement auprès de la banque des actes notariés. Cette banque fait office de source authentique pour les actes qui y sont enregistrés. Elle devra non seulement conserver les actes, mais aussi veiller à ce que ceux-ci restent lisibles et que leur intégrité ne puisse être atteinte, quelles que soient les évolutions de la technologie²². En outre, les notaires ont également la possibilité d'adresser à la banque des actes notariés des copies dématérialisées d'actes reçus sur support papier. Dans ce cas, ils ne sont pas déchargés de la tâche de conservation de la minute. Tant les modalités pratiques de cette loi que son entrée en vigueur doivent être déterminées par arrêté royal. De nouvelles modifications de la loi de ventôse seront nécessaires pour rendre le texte parfaitement fonctionnel tant pour les actes électroniques que pour les actes sur support papier : suppression du mot « minute », absence de toute référence à la signature manuscrite ou aux renvois et apostilles en marge²³...

16. Cependant, cette modification importante n'autorise toujours pas l'acte notarié à distance. La difficulté ne réside pas tant dans l'acte lui-même, dont on conçoit bien qu'il pourrait prendre une forme dématérialisée, mais plutôt dans l'idée que cet acte pourrait être passé « à distance », les clients du notaire n'étant plus présents physiquement devant lui. Comment l'authenticité pourrait-elle encore revêtir son sens plénier, dès lors que le notaire ne peut plus réaliser de constatations *ex propriis sensibus*, mais de manière médiate, par l'intermédiaire d'un ordinateur? Comment le devoir de conseil du notaire peut-il trouver sa pleine expression dans ce cadre? Il paraît donc difficile d'envisager la conclusion d'un acte notarié électronique, sans qu'ait lieu, à un moment donné de sa confection, un contact physique entre un notaire et une des parties²⁴.

²¹ M.B., 19 mai 2009.

²² B. VAN OPSTAL et S. ROELAND, « Het notariaat in de elektronische wereld — De elektronische akte in de elektronische wereld », *T. Not.* 2010, pp. 395 et s., n° 3.3.

²³ P. VAN DEN EYNDE, « Le droit du notariat : d'une loi de réforme à l'acte dématérialisé », *Rev. not.*, 2011, pp. 815 et s., n° 8.

²⁴ E. JOLY-PASSANT, *L'écrit confronté aux nouvelles technologies*, Paris, L.G.D.J., 2006, n° 72 et s., n° 754 et 755; C. LAZARO, « L'acte authentique à l'épreuve des nouvelles technologies », *Ubiquité*, 2002/13, pp. 7 et s., spéc. p. 29; B. VUYLSTEKE, « De elektronische authentieke akte », in *Elektronisch handel. Commentaar bij de wetten van 11 maart 2003*, Bruges, la Charte, 2003, pp. 187 et s., spéc. pp. 201-202. Une vidéoconférence, au cours de laquelle les deux parties seraient chacune assistée de son notaire pourrait constituer une amorce de solution à ce problème (E. JOLY-PASSANT, *op. cit.*, n° 753; J. TALPIS, « Nous devons réfléchir aux défis que pose le passage à l'acte notarié électronique », *Notarius*, 2009, pp. 30 et s.).

Section 3

Le courrier électronique

17. Autant les actes électroniques porteurs d'une véritable signature sont peu nombreux, autant la pratique voit s'échanger chaque jour des millions de messages non signés, par l'intermédiaire des systèmes de messagerie électronique. Il n'est donc pas rare que des versions imprimées de courriels soient produites en justice par les parties à un litige. Se pose alors la question de la force probante de ces messages.

La force probante d'un courriel ordinaire, ne portant pas de signature électronique, est fort dépendante de la définition des fonctions de l'écrit (*supra*, n° 3). En effet, le courrier électronique n'offre que peu de sécurité contre les falsifications de son contenu. Si on considère que l'inaltérabilité est une fonction essentielle de l'écrit, il faut bien reconnaître que l'e-mail n'y satisfait pas. Dans cette conception, l'e-mail ne peut donc être considéré comme un écrit et doit être rangé dans les présomptions. Sa valeur probante sera très dépendante des circonstances. Toutefois, le législateur n'a pas fait de l'inaltérabilité une caractéristique essentielle de l'écrit (*supra*, n° 4). Dès lors, le message électronique peut être admis parmi les écrits non signés²⁵.

S'agit-il d'un véritable commencement de preuve par écrit? Oui, s'il n'y a pas de contestation quant à son origine et que son auteur en admet la paternité. Dans la négative, l'absence de garanties offertes par le système quant à l'identification de l'auteur du message ne permet pas de considérer l'e-mail comme un commencement de preuve par écrit. Le même statut peut être réservé aux autres types de messages électroniques, notamment les messages écrits échangés entre téléphones portables (SMS)²⁶. Lorsque l'origine et le contenu du SMS ne font pas l'objet de discussion, ce type de message peut constituer un commencement de preuve par écrit²⁷.

La jurisprudence admet la preuve de faits par courriel lorsque l'existence et le contenu de ces messages ne sont pas contestés²⁸. En revanche, en cas de contestation, un courrier électronique est dépourvu de valeur probante, lorsqu'il a transité par un serveur interne du système informatique de la personne qui l'invoque, de telle sorte que celle-ci avait tout pouvoir de manipuler l'horloge

²⁵ Les références antérieures à la loi de 2003 qui adoptaient une position contraire (L. CORNELIS et P. GOETHALS, « Contractuele aspecten van e-commerce », in *Le droit des affaires en évolution. Le commerce électronique*, Bruxelles, Bruylant-Kluwer, 1999, pp. 1 et s., spéc. p. 32) ne sont plus d'actualité.

²⁶ D. GOBERT et E. MONTERO, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, 2001, p. 128.

²⁷ Civ. Gand, 10 avril 2012, *Juristenkrant*, 2012, n° 248, p. 1.

²⁸ C. trav. Gand (sect. Bruges), 23 septembre 2003, *J.T.T.*, 2004, p. 334.

du système ainsi que les journaux des opérations effectuées par le système²⁹. La question de la valeur probante d'un courrier électronique adressé via un serveur mail public, placé sous le contrôle d'un tiers, n'a pas encore été tranchée. Dans tous les cas, une expertise permettrait d'obtenir un avis sur la réalité et la date de l'envoi du courrier, mais encore faut-il que les frais d'une telle mesure soient en proportion avec l'enjeu du litige³⁰.

Section 4

Preuve du contenu d'un site web

18. Un des problèmes posés par internet au niveau de la preuve est la fugacité des informations. Le contenu d'un site web peut être modifié d'heure en heure. Des pages web peuvent disparaître purement et simplement ou être totalement bouleversées. Rien ne dit que les conditions générales d'un prestataire un jour étaient identiques la veille. Avec le développement du commerce et des relations contractuelles dans un environnement électronique, il peut être utile de conserver des traces d'informations diffusées sur internet : contenu d'une publicité, de conditions générales ou d'une offre, informations calomnieuses ou contrefaisantes, informations faisant l'objet d'un ordre de cessation, etc.

Le problème de la versatilité de l'information sur internet est difficile à gérer et ne connaît pas encore de solution organisée. Il est possible de faire appel à un tiers de confiance qui archiverait des pages web et pourrait certifier leur contenu. Mais ce procédé est davantage accessible au prestataire qu'à son client. En outre, il est encore peu répandu.

Les huissiers sont de plus mis à contribution pour opérer des constats du contenu de sites web. Ces constats doivent respecter des exigences techniques précises, à peine de quoi ils risquent d'être écartés.

Ces constats ont la même force probante que tous les autres constats d'huissier dressés à la requête de particuliers. Ils valent comme simples renseignements, sans préjudice toutefois de la valeur morale qui s'attache à l'intervention d'un huissier de justice³¹. Toutefois, s'y ajoutent des considérations techniques qui peuvent amener à invalider le constat, indépendamment de la rigueur et de la bonne foi de l'huissier instrumentant.

²⁹ Gand, 10 mars 2008, D.A.-O.R., 2009, liv. 91, p. 314, note E. MONTERO; *Digital evidence and electronic signature law review*, 2008, p. 99, note VAN ECKE et VERBRUGGE. Ceci pose la question de l'application de l'adage « nul ne peut se fournir de preuve à lui-même ».

³⁰ E. MONTERO, « À propos de la valeur probante des e-mails », D.A.-O.R., 2009, pp. 316 et s., spéc. 318.

³¹ D. et R. MOUGENOT, *op. cit.*, n° 244-2.

Ce contentieux est encore balbutiant en Belgique, mais la jurisprudence française, plus avancée sur ce point, a déjà permis d'élaborer un certain nombre de règles minimales à observer³².

Pour éviter toute contestation quant à la valeur technique de son constat, l'huissier veillera à :

- effectuer autant que possible le constat à partir de son ordinateur, plutôt que de celui de son client; cela évitera que le client ne configure l'ordinateur à l'insu de l'huissier, de façon à faire constater des choses qui n'existent pas;
- noter le type d'ordinateur, de système d'exploitation et de navigateur (*browser*); l'indication du navigateur est capitale, parce que les sites web ne se présentent pas de la même manière avec tous les navigateurs;
- indiquer son adresse IP, c'est-à-dire l'adresse qui lui est attribuée par le fournisseur d'accès à internet; cette donnée est capitale, parce que, en cas de contestation, elle permettra de vérifier que l'ordinateur de l'huissier a bien accédé au site web litigieux³³;
- vider la mémoire cache de son ordinateur, autre recommandation capitale; la mémoire cache conserve des pages déjà téléchargées; en cas de nouvelle consultation, pour plus de rapidité, l'ordinateur charge la page dans la mémoire cache plutôt que la page présente sur le web; si la page web a été modifiée entre-temps, le contenu de la page conservée dans la mémoire cache peut fort bien ne plus être conforme à celui de la page accessible sur internet, ce qui ôte toute valeur probante au constat;
- indiquer s'il accède à internet par un serveur *proxy*, c'est-à-dire un serveur intermédiaire, qui peut aussi conserver en mémoire des pages web qui ne correspondent plus à la réalité.

De manière générale, si l'huissier n'est pas sûr de ses compétences techniques, il est judicieux qu'il s'entoure des conseils d'un informaticien.

³² Voy. sur cette question : R. CARRAL et F. GUENIN, « Assurer l'efficacité des constats d'huissier sur le web : recommandations pratiques et juridiques », *Gaz. Pal.*, 2004, doctr., pp. 1686 et s.; A. PENNEAU, « Les nouveaux défis du droit de la preuve : contentieux contractuel et preuve des faits électroniques », in *Les nouveaux défis du commerce électronique*, Paris, L.G.D.J., 2010, pp. 71 et s.; T. VAN CANNEYT et C. VERDURE, « La validité des constats d'huissier relatifs à des sites internet », *R.D.T.I.*, 2009, pp. 47 et s.; T. VAN CANNEYT et C. VERDURE, « Bailiffs on the internet and the validity of their certified reports : lessons learned from the french and belgian courts », *Digital Evidence and Electronic Signature Law Review*, 2010, pp. 71 et s.

³³ R. Carral et F. Guenin (*op. cit.*, p. 1688) considèrent que cette mention est inutile, parce que la force probante du constat d'huissier suffit à rapporter une telle preuve. Il y a lieu de rappeler que ce n'est pas la bonne foi de l'huissier qui est mise en cause, mais le fait que, trompé par son mandant, il se pourrait qu'il n'accède pas réellement au site web dont le contenu doit être constaté. Les mêmes auteurs rappellent qu'il est parfaitement possible de reconstituer un site web sur un réseau local, donnant l'illusion à l'utilisateur qu'il est en train de naviguer sur un vrai site web. D'où l'importance, pour l'huissier, d'opérer son constat sur son ordinateur, et non celui de son client.

La sanction du non-respect de ces recommandations dans la jurisprudence française est l'écartement pur et simple du constat, pour défaut de valeur probante. Toutefois, si un premier constat s'avère inopérant, un constat ultérieur permet de corriger les irrégularités, si les pages web litigieuses sont toujours accessibles sur un site d'archivage³⁴.

Section 5

La preuve par l'image (films et photographies)

§ 1. Nature juridique

19. Si l'on excepte la photographie d'un document qui est assimilable à une photocopie, les films et photographies ne peuvent normalement servir qu'à prouver des faits. Sur un plan juridique, photos et films constituent des présomptions de l'homme³⁵. Comme les faits, même en matière civile, peuvent être prouvés par toutes voies de droit, il n'existe pas d'objection de principe à la production en justice de photographies ou de films. Toutefois, le débat ne se placera pas uniquement sur le terrain de la valeur probante de ces mécanismes, mais aussi de leur admissibilité. Il se peut, en effet, que ces preuves soient écartées, non pas parce qu'elles ne prouvent rien, mais parce qu'elles violent la loi ou le droit au respect de la vie privée.

§ 2. Respect du droit à la vie privée

20. Il faudra, le cas échéant, veiller au respect de la vie privée des personnes³⁶. Ce concept est très extensif et ne s'arrête pas aux seuls lieux privés. Il protège également le droit à l'identité et au développement personnel, ainsi que le droit pour tout individu de nouer et de développer des relations avec ses semblables et le monde extérieur. Il peut aussi s'étendre aux activités relevant de la sphère professionnelle ou commerciale. Il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la « vie privée »³⁷. La vie privée n'est plus limitée à son sens étroit de stricte intimité de la personne, mais exprime la liberté des choix de vie de l'individu contribuant à

son plein épanouissement. Le droit à la vie privée ne s'évanouit donc pas du seul fait que l'individu se trouve placé sous le regard d'autrui³⁸. Il est donc réducteur de considérer que les photos prises dans des lieux publics ne peuvent, par principe, porter atteinte à la vie privée de la personne photographiée³⁹.

Ceci dit, la vie privée n'est pas un concept absolu. L'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution autorisent des ingérences dans la vie privée pour autant que trois conditions soient respectées :

- l'auteur de l'atteinte doit agir en exécution d'une loi (légalité) ;

Ce terme ne doit pas s'entendre dans un sens trop strict. Il n'est pas nécessaire, dans le cadre de l'application de l'article 8, C.E.D.H., que la pratique concernée soit prévue par une loi, au sens formel du terme⁴⁰. Il suffit qu'elle soit conforme au droit, en général, quelle qu'en soit la source. Ce peut être un principe jurisprudentiel. Ce qui importe, c'est que l'ingérence dans la vie privée soit autorisée par une norme qui est accessible et prévisible⁴¹. L'article 22 de la Constitution est à cet égard plus contraignant, puisque seul le législateur est investi du pouvoir de faire respecter la vie privée. En droit interne, il faut donc une loi, au sens strict, pour autoriser une exception à ce principe⁴².

- l'ingérence doit se faire en application d'un « besoin impérieux »⁴³ (légitimité) ;

Selon l'article 8, alinéa 2, C.E.D.H., il doit s'agir d'une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

- l'atteinte doit être limitée au strict nécessaire (proportionnalité).

³⁸ J. MOULY, « Vie professionnelle et vie privée. De nouvelles rencontres sous l'égide de l'article 8 de la convention européenne », in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, F. SUDRE (dir.), Bruxelles, Bruylant, Nemesis, 2005, p. 280.

³⁹ N. VAN LEUVEN, « Het bewijs in echtscheidingsprocedures in het licht van het recht op eerbiediging van het privé-leven », *Echts. J.*, 2003, pp. 12 et s., n° 7.

⁴⁰ B. DOCCQUIR, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, n° 191 ; J.-Fr. NEVEN, « Les principes généraux : les dispositions internationales et constitutionnelles », in *Vie privée du travailleur et prérogatives patronales*, Bruxelles, éd. Jeune Barreau, 2005, pp. 36 et s., n° 16.

⁴¹ C.E.D.H., 26 avril 1979, *Sunday Times c. Royaume-Uni*.

⁴² C. arb., 19 juillet 2005, arrêt 131/2005, *Arr. C.A.*, 2005, p. 1719 ; M.B., 8 août 2005, p. 34459 ; *Juristenkrant*, 2005, p. 17 ; *J. dr. jeun.*, 2005, p. 63 ; *Rev. dr. étr.*, 2005, p. 375 ; *J. dr. jeun.*, 2006, p. 26, note C. VAN ZEEBROECK ; T.B.P., 2006, p. 487 ; T.J.K., 2006, p. 120 et 2007, p. 59, somm. ; R.W., 2006-2007, p. 209, somm.

⁴³ Voy. notamment l'expression revient fréquemment dans la jurisprudence de la Cour : C.E.D.H., 22 octobre 1981, *Dudgeon c. Royaume-Uni* ; C.E.D.H., 19 février 1998, *Dalia c. France* ; C.E.D.H., 2 août 2001, *Boultif c. Suisse* ; C.E.D.H., 9 octobre 2003, *Slivenko c. Lettonie* ; C.E.D.H., 4 décembre 2008, *S. et Marper c. Royaume-Uni*.

³⁴ T. VAN CANNEYT et C. VERDURE, « Constats d'huissier et sites internet : le recours aux sites d'archivage est-il la solution miracle ? », *R.D.T.I.*, 2011, pp. 108 et s. Les auteurs critiquent une décision du Tribunal de grande instance de Paris du 27 mai 2011, qui a écarté de manière assez abrupte un constat réalisé sur la base de pages archivées par un site privé. Ce jugement est publié dans le même numéro de cette revue, p. 99.

³⁵ L. CORNELIS et L. SIMONT, *op. cit.*

³⁶ H. DE PAGE, *Traité élémentaire de droit civil belge*, t. II, vol. 1, 4^e éd., par J.-P. MASSON, Bruxelles, Bruylant, n° 49 et s. ; *Civ. Bruxelles*, 27 novembre 1993, *J.L.M.B.*, 1994, p. 1001.

³⁷ C.E.D.H., 17 juillet 2003, *Perry c. Royaume-Uni* ; voy. aussi : C.E.D.H., 4 mai 2000, *Rotaru c. Roumanie* ; C.E.D.H., 16 février 2000, *Amann c. Suisse*.

Le lecteur sera par ailleurs attentif à l'incidence sur cette question de la loi du 8 décembre 1992 relative à la protection de la vie privée contre les traitements de données à caractère personnel. Si la photo est prise à l'aide d'un appareil photo numérique, ce procédé suffit pour que la prise de photos soit assimilée à un traitement automatisé et soit donc soumise à cette loi⁴⁴. En revanche, il n'y a pas de traitement automatisé si les photos sont prises avec un appareil classique, où la photo est réalisée par l'exposition d'un support argentique. C'est l'utilisation de ces photos qui est alors importante : si ces photos sont organisées et conservées en suivant une structure logique permettant une consultation systématique, on pourra parler de fichier et la loi s'appliquera quand même.

Même si la prise de vue peut être considérée comme attentatoire à la vie privée ou contraire à la loi, il ne faut pas perdre de vue l'évolution de la jurisprudence en matière d'utilisation de preuves illicites (jurisprudence *Antigone*, voy. l'exposé de Nathalie Colette-Basecqz et de Ilheme Bekhouche dans le présent ouvrage). On retiendra que, dans le cadre de cette jurisprudence, les preuves illicites pourront être écartées lorsque l'irrégularité affecte la valeur probante du moyen de preuve. Dans le cas de la photo, la fragilité du mode de preuve liée à la possibilité de trucage est inhérente au procédé utilisé et non à l'irrégularité de la prise de vue. Donc, même si une photo est prise dans le strict respect de la vie privée de la personne photographiée, le doute lié à la possibilité de traitement de la photo subsiste.

§ 3. Force probante – Valeur probante

21. La valeur probante de photographies ou de films est, comme toujours en matière de présomptions, appréciée souverainement par le juge. Celui-ci veillera à écarter les documents soupçonnés de trucage. Il se méfiera des impressions fallacieuses résultant de l'angle de prise de vues ou de l'éclairage employé. Le développement des logiciels de traitement d'image (*photoshop* ou autre) a encore accru les possibilités de retoucher une photographie. Le juge s'interrogera également sur la date à laquelle les épreuves ont été réalisées⁴⁵. Des témoignages ou des interventions d'huissiers de justice peuvent à cet égard se révéler utiles.

L'appréciation souveraine du juge du fond a cependant ses limites. Il ne pourrait donner à une photographie une interprétation inconciliable avec son contenu, car, dans cette hypothèse, la censure de la Cour de cassation aurait à s'exercer⁴⁶.

§ 4. Caméras de surveillance

22. La pose de caméra de surveillance est désormais réglementée par la loi du 21 mars 2007. Les commentaires qui suivent seront très succincts, et nous renvoyons le lecteur désireux d'informations plus précises à la doctrine spécialisée⁴⁷.

On entend par caméras de surveillance des caméras fixes⁴⁸ destinées à prévenir, constater ou déceler des délits contre les personnes ou les biens, les nuisances au sens de l'article 135 de la loi communale ou à maintenir l'ordre public (article 2). La loi ne vise donc pas la prise de vue par caméra réalisée en vue de toute autre finalité. L'installation d'une caméra de surveillance dans un lieu ouvert ne peut être effectuée qu'après avis positif du Conseil communal (article 5). L'installation d'une caméra de surveillance dans un lieu fermé, accessible ou non au public, ne peut être effectuée qu'après déclaration à la Commission de la vie privée et au chef de zone de police (articles 6 et 7). Ces dispositions ne s'appliquent pas aux caméras installées par une personne physique à des fins personnelles ou domestiques (article 7, § 2). Lorsqu'une caméra de surveillance est installée, sa présence doit être matérialisée par un pictogramme adapté (article 6, § 2, et article 7, § 2).

L'utilisation cachée de caméras de surveillance, c'est-à-dire sans consentement préalable de la personne filmée, est interdite (article 8). Le fait de pénétrer dans un lieu où est placé le pictogramme adéquat équivaut à une autorisation. Les caméras ne peuvent fournir des données touchant à l'intimité de la personne ou dites sensibles (relatives à ses opinions philosophiques, religieuses, politiques ou syndicales, à son origine ethnique ou sociale, à la vie sexuelle ou à l'état de santé) (article 9).

La surveillance par vidéo sur les lieux du travail fait l'objet d'une réglementation particulière, prévue à la Convention collective de travail n° 68 du 16 juin

⁴⁴ Cass., 29 janv. 1985, *Pas*, 1985, I, p. 626.

⁴⁵ Voy. à ce sujet : B. DOCQUIR, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, n° 709 et s. ; F. DELPERÉE, « La protection de la vie privée et les caméras de vidéosurveillance », in *Vigilantibus ius scriptum. Feestbundel voor Hugo Vandenberghe*, Bruges, la Chartre, 2007, pp. 109 et s. ; F. DUMORTIER, « La vidéosurveillance sous l'angle de la proportionnalité. Premières réflexions au sujet de la loi réglant l'installation et l'utilisation de caméras de surveillance », *R.D.T.I.*, 2007, pp. 311-350 ; P. VAN EECHE et B. OOMS, « De nieuwe wet op de camerabewaking : een analyse van een langverwachte wet na een rechtsonzekere periode », *Computerr*, 2008, pp. 147-160.

⁴⁶ La loi réglemente aussi l'utilisation de caméras mobiles de surveillance, mais celles-ci ne peuvent être utilisées que par les forces de police (art. 7/1 et 7/2).

⁴⁴ P. DE HERT, « Données à caractère personnel et caméras », in *Manuel de la vie privée*, Bruxelles, Politeia, feuillets mobiles, p. 49 (2) ; W. VAN LAETHEM, « Mogelijkheden en beperkingen bij het afuisteren en bespieden door privédetectives », in *Ontwikkeling inzake private opsporing*, Anvers, Maklu, 2002, pp. 89 et s., spéc. p. 91.

⁴⁵ Voy. G.-L. BALLON, *Het bewijs en de moderne technieken*, Centrum voor beroepsvervolmaking in de Rechten, Anvers, 1989, p. 14, n° 20, 1.

1998 relative à la protection de la vie privée à l'égard de la surveillance par caméra sur le lieu du travail⁴⁹.

Section 6

La preuve par le son

§ 1. Nature juridique

23. Les enregistrements magnétiques sont actuellement supplantés par les enregistrements numériques, qui peuvent être stockés sur tout support numérique (disque dur, CD, DVD, clé USB, etc.). Le procédé n'a toutefois que peu d'incidence sur la valeur juridique des enregistrements. Ce qui a été dit pour les enregistrements magnétiques est transposable pour les enregistrements numériques. À deux reprises, notre Cour de cassation a décidé que de tels enregistrements pouvaient constituer des présomptions⁵⁰. La doctrine presque unanime adopte cet enseignement⁵¹. En Belgique, quelques auteurs défendent l'idée que l'enregistrement constituerait un commencement de preuve par écrit⁵². L'élargissement de la notion d'écrit a donné plus de crédit à cette thèse. La doctrine classique commande cependant de s'en tenir à la notion de présomption⁵³.

⁴⁹ Rendue obligatoire par arrêté royal du 20 septembre 1998 (M.B., 2 octobre 1998, p. 32486). Voy. à ce sujet : B. DOCKRUIJ, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, n° 757 et s. ; E. CARLIER et G. ALBERT, « L'instauration d'un plan de sécurité dans l'entreprise et le droit au respect de la vie privée », in *Vie privée du travailleur et prérogatives patronales*, Bruxelles, éd. Jeune Barreau, 2005, pp. 187 et s. ; S. GILSON, K. ROSIER et E. DERMINE, « La preuve en droit du travail », in *La preuve. Questions spéciales*, Formation permanente CUP, vol. 99, Liège, Louvain-la-Neuve, Anthémis, 2008, pp. 179 et s., n° 74 et s. ; F. DUMORTIER, « La surveillance par caméras : de la supervision de lieux vers l'observation systématique de personnes », in *Discipline et surveillance dans la relation de travail*, Limal, Anthémis, 2013, pp. 333 et s.

⁵⁰ Cass., 24 novembre 1961, *Pas.*, 1962, I, p. 367 ; Cass., 29 octobre 1962, *Pas.*, 1963, I, p. 272. Voy. aussi Comm. Bruxelles, 16 décembre 1980, J.C.B., 1981, p. 151.

⁵¹ VAN RYN et HEENEN, t. III, 2^e éd., n° 57 ; P. VAN OMMESSLAGHE, implicitement, « Les obligations. Examen de jurisprudence (1974-1982) », R.C.J.B., 1988, p. 172 ; L. CORNELIS et L. SIMONT, « Bewijsrecht en technologische evolutie. Enkele overwegingen », in *Recht en technologie*, Anvers, Kluwer, 1987, pp. 150 et s. ; R. MATTHYS, « Geluidstechniek in burgerlijk procesrecht en strafprocesrecht », R.W., 1963-1964, col. 584 ; D. MATTHYS, « La vie privée et le droit de la preuve en matière civile », *Ann. dr.*, 1984, p. 392.

⁵² M. FONTAINE, « La preuve des actes juridiques et les techniques nouvelles », in *La preuve*, Colloque UCL, 1987, p. 27 ; R. ABRAHAM, « La preuve civile par magnétophone », J.T., 1963, p. 585.

⁵³ L. CORNELIS et L. SIMONT, « Bewijsrecht en technologische evolutie. Enkele overwegingen », in *Recht en technologie*, Anvers, Kluwer, 1987, p. 151 ; Civ. Liège (réf.), 9 octobre 1991, *Pas.*, 1992, III, p. 112 ; P. VAN OMMESSLAGHE, « Introduction – Cadre légal – Notions fondamentales », in P. VAN OMMESSLAGHE (coord.), *Incidence des nouvelles technologies de la communication sur le droit commun des obligations*, formation permanente UB³, Bruxelles, Bruylant, 2012, pp. 1 et s., n° 19, note 46.

§ 2. Peut-on considérer un enregistrement sonore comme un aveu extrajudiciaire ?

24. Suivant L. Cornelis et L. Simont⁵⁴, il faut distinguer l'aveu verbal lui-même, et son enregistrement, et ne pas perdre de vue la règle de l'article 1355 du Code civil.

Si un aveu verbal a fait l'objet d'un enregistrement, ce dernier doit être considéré comme une présomption de l'homme susceptible de prouver l'aveu lui-même. Mais l'article 1355 du Code civil interdit d'éluder l'exigence d'un écrit formulée par l'article 1341 du Code civil en prétendant prouver par toutes voies de droit un aveu verbal dans une matière où la liberté des preuves n'existe pas⁵⁵.

Il ne peut, dès lors, être admis de prouver par un enregistrement un aveu verbal relatif à une obligation qui, conformément à l'article 1341 du Code civil, aurait dû être prouvée par écrit⁵⁶.

§ 3. Admissibilité

25. La question de l'admissibilité en justice de la preuve par enregistrements sonores, tout particulièrement de conversations téléphoniques, est particulièrement délicate. Il s'agit d'une matière qui connaît une évolution importante, de telle sorte que la doctrine et la jurisprudence anciennes sont à prendre avec prudence. La jurisprudence a paru, durant un temps, faire la distinction entre les enregistrements réalisés en matière privée et ceux effectués en matière commerciale.

A. Les communications privées

26. La première question à se poser est de déterminer si l'enregistrement produit n'était pas purement et simplement interdit par la loi. Outre l'interdiction de la divulgation de données couvertes par le secret professionnel⁵⁷, il faut tenir compte, sur ce point, des législations sur la protection des conversations téléphoniques et des communications électroniques.

Le Code pénal interdit l'écoute et l'enregistrement intentionnels de communications et télécommunications privées par tout officier ou fonctionnaire public

⁵⁴ L. CORNELIS et L. SIMONT, *op. cit.*, pp. 150 et s. ; *contra*, mais à tort, J.P. Fexhe-Slins, 28 mai 1958, *Jur. Liège*, 1958-1959, p. 14.

⁵⁵ H. DE PAGE, *op. cit.*, t. III, 3^e éd., n° 1026 ; J.-L. MOURALIS, *La Preuve*, Rép. *dr. civ. Dalloz*, 2^e éd., 2002, n° 780 et s.

⁵⁶ Civ. Bruxelles, 11 décembre 1992, J.J.P., 1994, p. 121.

⁵⁷ B. ALLEMEERSCH et P. SCHOLLEN, « Behoorlijk bewijs in burgerlijke zaken. Over de geoorloofde vereiste in het burgerlijk bewijsrecht », R.W., 2002-2003, pp. 41 et s., spéc. p. 43.

ou dépositaire ou agent de la force publique (article 259bis) ou par quiconque (article 314bis), pour autant qu'ils ne prennent pas part à la conversation⁵⁸. La première disposition interdit donc les écoutes téléphoniques non autorisées par les autorités, la seconde les écoutes et les enregistrements téléphoniques réalisés par de simples particuliers, qui ne participent pas à la conversation.

L'article 124 de la loi du 13 juin 2005 relative aux communications électroniques interdit à quiconque de prendre intentionnellement connaissance de l'existence d'une information transmise par voie électronique, ainsi que de l'identité des personnes concernées, pour autant que cette communication ne lui soit pas destinée personnellement⁵⁹. Il est également interdit de modifier, supprimer, révéler, stocker ou faire un usage quelconque de ces informations, même si celles-ci n'ont pas été obtenues de manière intentionnelle. La loi distingue donc l'interception des données, qui doit être intentionnelle, et la conservation et l'utilisation des données, qui peut également viser des données connues par accident. Le cadre réglementaire européen donne une définition très large des services de communication électronique, dans la mesure où il entend établir un principe de neutralité technologique. Les services de communication consistent à transmettre ou à acheminer des signaux sur un réseau de communications. Dès lors, la loi du 13 juin 2005 englobe désormais le service de téléphonie vocale dans la notion de « service téléphonique accessible au public. »⁶⁰

Il ressort donc de ces différentes dispositions une interdiction générale de prendre connaissance et d'enregistrer des communications auxquelles on ne participe pas ou dont on n'est pas destinataire.

En revanche, il n'est pas interdit d'enregistrer une conversation à laquelle on prend part. Et c'est cette question qui pose problème dans la plupart des cas. Classiquement, doctrine et jurisprudence se sont montrées très réticentes à admettre ce type d'enregistrement, sans autorisation du ou des correspondants. Les griefs habituellement soulevés étaient la déloyauté du procédé et l'atteinte à la vie privée du correspondant. Tout enregistrement obtenu de manière déloyale au moyen d'un appareil dissimulé dans un local, un appartement et, *a fortiori*, dans un vêtement était en principe rejeté. C'est le cas pour un enregistrement réalisé de manière clandestine par un huissier de justice dissimulant un appareil

⁵⁸ Voy. Th. HENRIOT, « Les écoutes téléphoniques », *J.T.*, 1995, pp. 205 et s.

⁵⁹ Quiconque prend connaissance du contenu d'un courriel ne peut le faire sans prendre connaissance simultanément de son existence et viole donc l'article 124, 1^{er}, de la loi du 13 juin 2005 (Cass., 1^{er} octobre 2009, *Pas.*, 2009, p. 2063; *Larc. Cass.*, 2010, p. 16, n° 56, somm.; *J.R./D.J.*, 2010, p. 399, note B. PONET; *Limb. Rechtsl.*, 2010, p. 77, note B. PONET; *R.W.*, 2010-2011, p. 322).

⁶⁰ F. DEHOUSSE et T. ZGAJEWSKI, « Le nouveau régime des communications électroniques en Belgique à la suite de la loi du 13 juin 2005 », *J.T.*, 2006, pp. 537 et s., spéc. p. 542.

portatif⁶¹. D'une manière générale, on prohibait aussi la production de l'enregistrement d'une conversation téléphonique réalisée à l'insu de l'interlocuteur⁶². La jurisprudence récente se montre plus nuancée. À côté de décisions qui écartent ce mode de preuve par principe⁶³, on en trouve d'autres qui font une analyse plus fine des circonstances qui entourent la création de l'enregistrement. Tout d'abord, il n'y a aucune atteinte à la vie privée de l'appelant lorsque le destinataire de l'appel enregistre la communication. C'est ce que la Cour de cassation a admis, en matière pénale, dans les termes suivants : « celui qui tient une conversation téléphonique ne peut invoquer le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance, mentionné aux articles précités, à l'égard de l'intervenant à cette conversation, faisant lui-même participer cet intervenant à l'objet de ce droit »⁶⁴. Rien n'empêche donc que le destinataire de l'appel enregistre des injures ou des menaces proférées par téléphone⁶⁵.

Même lorsque c'est l'appelant qui enregistre la conversation, la jurisprudence est de plus en plus sensible aux circonstances de l'affaire pour décider si ce mode de preuve est admissible ou non. La Cour de cassation a reconnu que le seul fait d'enregistrer une conversation à laquelle on participe soi-même n'est pas illicite, même si cet enregistrement est fait à l'insu des autres participants. Il faut donc vérifier au cas par cas s'il y a violation du droit au respect de la vie privée⁶⁶. S'il est vrai que les propos tenus au téléphone relèvent de la vie privée du correspondant, le principe du respect de la vie privée se heurte ici au principe

⁶¹ Civ. Bruxelles, 7 mai 1958, *J.T.*, 1958, p. 364; J. RUTSAERT, « Le système jurisprudentiel du droit au respect de la vie privée », *J.T.*, 1973, p. 493; L. CORNELIS et L. SIMONT, « Bewijsrecht en technologische evolutie. Enkele overwegingen », in *Recht en technologie*, Anvers, Kluwer, 1987, pp. 162 et s.; D. MATTHYS, « La vie privée et le droit de la preuve en matière civile », *Ann. dr. Louvain*, 1984, p. 392; *adde* Cass. fr., 20 novembre 1991, D.-S., 1992, jur., p. 93.

⁶² H. DE PAGE, *op. cit.*, t. II, vol. I, 4^e éd. par J.-P. MASSON, n° 56; J. RUTSAERT, *op. cit.*, p. 492; A. FETTWEIS, *Manuel de procédure civile*, *op. cit.*, n° 476, B. 3; J. DE LIEDEKERKE, « La protection de la personnalité en droit privé belge », *J.T.*, 1959, p. 415, n° 25; R. MATTHYS, « Geluidstechnieken in burgerlijk procesrecht en strafprocesrecht », *R.W.*, 1963-1964, col. 587; D. HUET-WEILLER, « La protection juridique de la voix humaine », *Rev. trim. dr. civ.*, 1982, p. 497; Anvers, 13 mars 1991, *Bull. ass.*, 1991, p. 867; Comm. Bruxelles, 7 mai 1991, *J.T.*, 1991, p. 568, décision dont la motivation a été nuancée en degré d'appel (Bruxelles, 15 mars 1994, *J.T.*, 1994, p. 657 et note critique F. RIGAUX); Civ. Turnhout, 20 octobre 1977, *Rev. dr. fam.*, 1978, p. 292; Comm. Ypres, 20 novembre 1995, R.D.C., 1996, p. 1007; Paris, 15 mai 1998, D., 1998, inf. rap., 1996.

⁶³ Anvers, 4 avril 2001, A.J.T., 2001-2002, p. 767; Pol. Bruges, 15 septembre 2005, D.A.-O.R., 2007, p. 328.

⁶⁴ Cass., 9 janvier 2001, *Pas.*, 2001, I, p. 31; *Computerr.*, 2001, p. 199, note DUMORTIER; *Jaarboek Mensenrechten*, 2000-2001, p. 275, note DE HERT; T. Strafr., 2001, p. 335; *Vigiles*, 2001, p. 145, note VERSPELT.

⁶⁵ S. BOULART, « De opname van eigen telefoongesprekken : met of zonder toestemming van de betrokkenen ? », *R.W.*, 2002-2003, pp. 1601 et s., n° 60. Ce procédé avait été condamné par un arrêt de la Cour de cassation de France assez ancien (J. RUTSAERT, *op. cit.*, p. 493; R. SAVATIER, « Bandes magnétiques », note sous Cass. fr., 18 mars 1955, D., 1955, jur., p. 573).

⁶⁶ Cass., 9 septembre 2008, *Pas.*, 2008, p. 1889, concl. M. Timperman; *Rev. trim. dr. fam.*, 2010, p. 1030, somm.; *Chron. D.S.*, 2010, p. 547, somm. et concl. M. Timperman.

du droit à la preuve de son adversaire⁶⁷. Pour rappel, une partie a en principe le droit de produire dans une instance les preuves dont elle dispose. Lorsque ce droit entre en conflit avec un autre droit fondamental d'égale valeur, comme le droit au respect de la vie privée, le juge doit alors procéder à un arbitrage.

Les critères proposés par la jurisprudence pour retenir des enregistrements réalisés à l'insu du correspondant sont notamment : le fait que les déclarations enregistrées ont été faites spontanément et n'ont pas été encouragées ou provoquées ; la circonstance que le fait à prouver n'aurait pas pu être établi d'une autre manière⁶⁸.

B. Les communications commerciales

27. Si la doctrine classique se montrait très réservée quant à l'utilisation d'enregistrements de conversations privées, cette réticence était moins marquée dans le domaine des affaires, au motif que, dans cette matière, les communications n'avaient pas le même caractère confidentiel. On admettait volontiers que la conversation entre commerçants relative à la conclusion d'un marché n'avait rien de confidentiel⁶⁹. En revanche, s'il s'agissait de deux personnes qui se trouvaient en conflit, il convenait, même s'il s'agissait de commerçants, de se montrer très prudent. En effet, il n'est nullement impossible que l'un des interlocuteurs tente de manipuler son correspondant pour le piéger.

Cette différence de statut entre communications purement privées et communications d'affaires n'est, en réalité, guère justifiée. En effet, la Cour européenne des droits de l'homme considère que la protection de la vie privée s'étend également au domaine professionnel⁷⁰. Elle peut y prendre la forme de la protection du secret des affaires⁷¹.

Par ailleurs, une certaine confiance doit exister entre partenaires commerciaux, qui peut être ruinée si des enregistrements de conversations sont réalisés à l'insu de l'autre partie. Il convient toutefois de mettre cette considération en balance avec le comportement adopté par l'adversaire dans le cadre de l'administration

⁶⁷ Gand, 16 février 2010, T.G.R.-T.W.V.R., 2010, p. 258 ; NjW, 2010, p. 546, note E. B. ; *Rev. trim. dr. fam.*, 2011, p. 227, somm. ; B. ALLEMEERSCH, « De heimelijke opname van een eigen (telefoon) gesprek als bewijs in burgerlijke en commerciële geschillen », D.A.-O.R., n° 83, 2007, pp. 333 et s., n° 5.

⁶⁸ Gand, 16 février 2010, cité à la note précédente ; Gand, 6 septembre 2006, D.A.-O.R., 2007, p. 326 ; *Comm. Courtrai*, 24 juin 2004, D.A.-O.R., 2007, p. 331.

⁶⁹ J. RUTSAERT, « Le système jurisprudentiel du droit au respect de la vie privée », J.T., 1973, pp. 489 et s., p. 493, n° 27 ; J.-L. MOURALIS, *v° Preuve*, *Rép. dr. civ. Dalloz*, 2^e éd., 2002, n° 1387 ; D. MATTHYS, *op. cit.*, *Ann. dr. Louvain*, 1984, p. 393 ; Dijon, 26 juin 1957, J.C.P., 1957, II, 10279.

⁷⁰ C.E.D.H., 16 décembre 1992, *Niemietz c. Allemagne*, J.T., 1994, p. 65, note E. JAKHIAN et P. LAMBERT ; R.U.D.H., 1993, p. 241 ; *Rev. trim. D. H.*, 1993, p. 467, note P. LAMBERT ; *Rev. trim. D. H.*, 1993, p. 467, note F. RIGAUX.

⁷¹ D. MOUGENOT, « Le secret des affaires et ses implications en droit judiciaire », R.D.J.P., 2009, pp. 112-117 ; P. KAYZER, « Les droits de la personnalité. Aspects théoriques et pratiques », *Rev. trim. dr. civ.*, 1971, pp. 445 et s., n° 35 ; B. DOCQUIR, *op. cit.*, n° 80 et s. ; B. ALLEMEERSCH, « Zakengeheim in burgerlijk proces en bewijs », in *Zakengeheim*, Coll. *Recht en onderneming*, vol. 41, Bruges, la Chartre, 2012, pp. 1 et s.

de la preuve. Celui qui adopte une attitude de dénégation complète et ne collabore pas loyalement à l'administration de la preuve obligera peut-être son cocontractant à recourir à des modes de preuve plus délicats, et les tribunaux pourront être sensibles à cette situation⁷².

Pour terminer, on peut relever la faculté offerte par la loi du 13 juin 2005 sur les communications électroniques d'enregistrer des communications comme preuve d'une transaction commerciale ou d'une autre communication professionnelle (article 128). Toutefois, les parties doivent être informées de l'enregistrement, des objectifs précis de ce dernier et de la durée de stockage des données avant que l'enregistrement soit réalisé.

Même si l'enregistrement est déclaré illicite ou déloyal, son sort n'est pas encore joué. Il convient alors de déterminer si l'irrégularité constatée suffit à l'écarter comme moyen de preuve. Nous renvoyons à ce qui est dit à ce sujet aux numéros 18 et suivants.

§ 4. Force et valeur probante des enregistrements

28. Le principe découle des exposés qui précèdent : la force probante des enregistrements est celle des présomptions en général. La valeur probante de l'enregistrement fait l'objet d'importantes réserves en raison des dangers de truchage, altérations, découpages, suppressions de passages ou surimpressions⁷³. Ces dangers n'ont fait que croître avec le développement de l'informatique, qui permet le traitement du son aussi bien de l'image. Il faut évidemment être attentif aux critiques éventuelles de celui dont la voix a été enregistrée et, s'il y a lieu, recourir à une expertise⁷⁴.

⁷² B. ALLEMEERSCH, « De heimelijke opname van een eigen (telefoon) gesprek als bewijs in burgerlijke en commerciële geschillen », *op. cit.*, n° 8.

⁷³ Voy., à cet égard, les auteurs cités ci-dessus, spéc. A. FETTWEIS, *Manuel de procédure civile*, *op. cit.*, n° 476, B, 3. M. FLAMÉE et M. TANGHE, « Bewijsrecht : beknopte status quaestionis », in *Le droit des affaires en évolution*, Bruxelles, Bruylant et Anvers, Kluwer, 1992, p. 207, n° 24 ; Civ. Charleroi, 14 novembre 1990, J.L.M.B., 1991, p. 107, n'admet la production de l'enregistrement qu'en raison d'un ensemble de présomptions en faveur de sa fiabilité ; *adde* Civ. Liège (réf.), 9 octobre 1992, J.L.M.B., 1994, p. 235.

⁷⁴ M. FONTAINE, *op. cit.*, in *La preuve*, Colloque UCL, 1987, p. 28 ; D. MATTHYS, *op. cit.*, *Ann. dr. Louvain*, 1984, p. 394.